Тумко Сергій Петрович,
аспірант Національної академії Служби безпеки України

ВИКОРИСТАННЯ КОШТІВ ПІД ЧАС ОПЕРАТИВНОЇ ЗАКУПІВЛІ

Негласні слідчі розшукові дії (далі -НСРД) за походженням є оперативно-розшуковими заходами, в основу яких покладено передбачену чинним законодавством, із використанням специфічних методів та засобів, послідовність процесуальних дій уповноважених суб'єктів, спрямованих на виявлення, розкриття та припинення протиправних посягань.

Основним функціональним призначенням НСРД є забезпечення оптимальних шляхів використання у кримінальному провадженні інформації, отриманої з використанням негласних сил, засобів та методів, які використовуються в оперативно-розшуковій діяльності.

Враховуючи суспільну небезпеку обігу товару, який обмежений чи заборонений чинним законодавством, існування такої НСРД, як контроль за вчиненням злочину у формі оперативної закупки є позитивним явищем у теорії та практиці кримінального процесу.

Слід врахувати, що діяльність, пов'язана з проведенням оперативної закупки, є однією з найбільш комплексних, яка потребує суворого дотримання законності, оскільки безпосередньо зачіпає права і свободи людини і громадянина, Вказана діяльність має бути відповідного, адекватного характеру і ступеню суспільної небезпеки злочинного посягання, співвідношення законності і гласності, конспіративності і відкритості, тотальності заходів та індивідуальності підходу до тієї чи іншої ситуації.

Зокрема, відповідно до постанови Верховного Суду від 01 липня 2020 року справа № 643/10749/14-к згідно з п. 2.10 «Інструкції про порядок оперативної закупівлі наркотичних засобів, психотропних речовин та прекурсорів» затвердженої наказом МВС України № 023/0134 для проведення оперативної закупівлі використовуються грошові кошти СБУ, МВС України та інші засоби. Їх отримання і використання здійснюється у відповідності з відомчими нормативними актами СБУ та МВС України. При цьому корінець платіжного доручення, від ВФРЕВ УМВС України у Харківській області, який би свідчив про видачу працівникам СУ ГУМВС України у Харківській області витрат спеціального призначення в цьому кримінальному провадженню для проведення оперативної закупівлі у ОСОБА_1 суду не надано, що є грубим порушенням кримінально-процесуального законодавства [1].

Таким чином суди дійшли обґрунтованого висновку, що при відсутності витрат спеціального призначення працівники СУ ГУМВС України об'єктивно не могли видати покупцю оперативної закупки

грошові кошти, що необхідні для проведення оперативної закупівлі у ОСОБА_1.

Крім того, судами також враховано, що органи поліції провівши оперативну закупку 26 березня 2014 року ОСОБА_1 не затримували і нічого у нього не вилучали, оскільки ні один зі свідків не бачив факту передачі наркотичних засобів.

Таким чином, Верховний Суд дійшов висновку, що надані стороною обвинувачення докази є недопустимими, оскільки отримані з істотним порушенням вимог кримінального процесуального закону.

Список використаних джерел

1. Постанова Верховного Суду від 01 липня 2020 року справа № 643/10749/14-к // Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Page/2.

Федоренко Оксана Анатоліївна,
молодший науковий співробітник наукової лабораторії з проблем протидії злочинності ННІ № 1 Національної академії внутрішніх справ

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ТА ПРИПИНЕННЯ КІБЕРЗАГРОЗ

Штучний інтелект (ШІ) та машинне навчання (МО) продемонстрували значний прогрес за останні роки, і їх розвиток сприяв широкому спектру корисних застосувань. Оскільки вони почали проникати у більш вразливі сфери, з'явилося більше побоювань щодо їх стійкості до кібератак. Як і будь-яка інша технологія, штучний інтелект (AI) та машинне навчання (ML) можна використовувати для загрози безпеці або для покращення її за допомогою нових засобів [1].

Програмне забезпечення, яке працює на наших комп'ютерах та інтелектуальних пристроях, може проявляти вразливі місця в сфері безпеки, які можуть бути використані хакерами. Потенційні наслідки мають великі масштаби і коливаються від безпеки особи до рівня нації чи регіону.

Штучний інтелект ідеально підходить для вирішення деяких з наших найскладніших проблем, і кібербезпека, безумовно, потрапляє в цю категорію. Збільшення кібератак і поширення пристроїв дозволяють використовувати машинне навчання і ШІ, автоматизуючи виявлення загроз і реагуючи більш ефективно, ніж традиційні програмні підходи [2]. Завданням штучного інтелекту має бути вдосконалення засобів безпеки, і перш за все, пришвидшення реагування на випадки, як тільки виявляється шкідливе програмне забезпечення.

Інструменти безпеки ШІ працюють над виявленням, прогнозуванням, обґрунтуванням, діянням та вивченням потенційних